

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer implemented method, in a data processing system, for detecting fraud, the computer implemented method comprising:

a plurality of steps performed by a processor in the data processing system, the plurality of steps comprising:

receiving a set of historical data stored in a customer behavior database;

identifying a plurality of control points in the set of historical data using a data analysis module, further comprising:

performing a statistical analysis on the set of historical data for identifying a plurality of outliers, wherein the plurality of outliers are identified by the statistical analysis as a set of significantly different data points in a distribution of the set of historical data; and

performing data mining techniques on ~~validating~~ the plurality of outliers to distinguish between a first set of outliers and a second set of outliers, wherein the first set of outliers are classified by the data mining techniques as ~~valid non-fraudulent~~ outliers and the second set of outliers are classified by the data mining techniques as ~~invalid fraudulent~~ outliers, and wherein the first set of outliers are identified as the plurality of control points;

building at least one data model based on the plurality of control points, further comprising:

generating a fence that passes through the plurality of control points to define a boundary between data points, wherein the fence comprises line segments connecting the plurality of control points to form a continuous line for the boundary, and wherein data points inside or on the boundary of the fence represent acceptable behavior and data points outside the boundary of the fence represent fraudulent behavior;

receiving a set of updated data, wherein the set of updated data includes a plurality of current data stored in the customer behavior database;

identifying one or more new control points based on the set of updated data using the data analysis module, further comprising:

performing a statistical analysis on the set of updated data for identifying an additional plurality of outliers, wherein the additional plurality of outliers are identified by the statistical analysis as an additional set of significantly different data points in a distribution of the set of updated data; and

performing data mining techniques on ~~validating~~ the additional plurality of outliers to distinguish between a third set of outliers and a fourth set of outliers, wherein the third set of outliers are classified by the data mining techniques as ~~valid non-fraudulent~~ outliers and the fourth set of outliers are classified by the data mining techniques as ~~invalid fraudulent~~ outliers, and wherein the third set of outliers are identified as the one or more new control points;

adjusting the at least one data model to form an adjusted fence, within the at least one data model, based on the one or more new control points, wherein the at least one data model is refined for a plurality of iterations, further comprising:

generating the adjusted fence that passes through the plurality of control points and the one or more new control points to define a new boundary between data points, wherein the adjusted fence comprises line segments connecting the plurality of control points and the one or more new control points to form a new continuous line for the new boundary, and wherein data points inside or on the new boundary of the adjusted fence represent acceptable behavior and data points outside the new boundary of the adjusted fence represent fraudulent behavior; and
verifying a transaction based on the adjusted fence.

2. (Previously Presented) The computer implemented method of claim 1, wherein the set of historical data includes at least one of demographic data, psychographic data, transactional data, and environmental data.

3. (Previously Presented) The computer implemented method of claim 1, wherein the plurality of outliers in the distribution of the set of historical data are identified by analyzing the historical data using statistical modeling, outlier analysis, and data mining algorithms.

4-6. (Canceled)

7. (Previously Presented) The computer implemented method of claim 1, wherein the set of updated data includes at least one of demographic data, psychographic data, transactional data, and environmental data.

8. (Previously Presented) The computer implemented method of claim 1, wherein generating the adjusted fence includes:

adding the one or more new control points to the adjusted fence.

9. (Previously Presented) The computer implemented method of claim 1, wherein generating the adjusted fence includes:

changing one or more of the plurality of control points to the one or more new control points in the adjusted fence.

10. (Previously Presented) The computer implemented method of claim 1, further comprising:

determining whether the adjusted fence, within the at least one data model, reached a steady state;

converting the adjusted fence to a static model in response to a determination that the adjusted fence reached the steady state; and

refining the at least one data model for an iteration of the plurality of iterations in response to a determination that the adjusted fence has not reached the steady state.

11. (Previously Presented) The computer implemented method of claim 10, wherein determining whether the adjusted fence reached a steady state includes:

determining a difference between the adjusted fence and a previous data model, within the at least one data model, to form a delta value; and
determining whether the delta value is less than a threshold.

12. (Previously Presented) The computer implemented method of claim 11, wherein the threshold is two standard deviations from a mean within a normal distribution of data.

13. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to detect fraudulent activity, said method steps comprising ~~A computer program product, in a computer readable medium, for detecting fraud, the computer program product comprising:~~

~~a plurality of instructions stored in the computer readable medium, wherein the plurality of instructions are adapted to cause a processor in a computer to perform steps comprising:~~

~~receiving a set of historical data stored in a customer behavior database;~~

~~identifying a plurality of control points in the set of historical data using a data analysis module, further comprising:~~

~~identifying a plurality of control points in the set of historical data using a data analysis module, further comprising:~~

~~performing a statistical analysis on the set of historical data for identifying a plurality of outliers, wherein the plurality of outliers are identified by the statistical analysis as a set of significantly different data points in a distribution of the set of historical data; and~~

~~performing data mining techniques on validating the plurality of outliers to distinguish between a first set of outliers and a second set of outliers, wherein the first set of outliers are classified by the data mining techniques as valid non-fraudulent outliers and the second set of outliers are classified by the data mining techniques as invalid fraudulent outliers, and wherein the first set of outliers are identified as the plurality of control points;~~

~~instructions for building at least one data model based on the plurality of control points, further comprising:~~

generating a fence that passes through the plurality of control points to define a boundary between data points, wherein the fence comprises line segments connecting the plurality of control points to form a line for the boundary, and wherein data points inside or on the boundary of the fence represent acceptable behavior and data points outside the boundary of the fence represent fraudulent behavior;

receiving a set of updated data, wherein the set of updated data includes a plurality of current data stored in the customer behavior database;

identifying one or more new control points based on the set of updated data using the data analysis module, further comprising:

- performing a statistical analysis on the set of updated data for identifying an additional plurality of outliers, wherein the additional plurality of outliers are identified by the statistical analysis as an additional set of significantly different data points in a distribution of the set of updated data; and
- performing data mining techniques on ~~validating~~ the additional plurality of outliers to distinguish between a third set of outliers and a fourth set of outliers, wherein the third set of outliers are classified by the data mining techniques as ~~valid non-fraudulent~~ outliers and the fourth set of outliers are classified by the data mining techniques as ~~invalid fraudulent~~ outliers, and wherein the third set of outliers are identified as the one or more new control points;

adjusting the at least one data model to form an adjusted fence, within the at least one data model, based on the one or more new control points, wherein the at least one data model is refined for a plurality of iterations, further comprising:

- generating the adjusted fence that passes through the plurality of control points and the one or more new control points to define a new boundary between data points, wherein the adjusted fence comprises line segments connecting the plurality of control points and the one or more new control points to form a new continuous line for the new boundary, and wherein data points inside or on the new boundary of the adjusted fence represent acceptable behavior and data points outside the new boundary of the adjusted fence represent fraudulent behavior; and
- verifying a transaction based on the adjusted fence.

14. (Currently Amended) The ~~computer program product~~ program storage device of claim 13, wherein the set of historical data includes at least one of demographic data, psychographic data, transactional data, and environmental data.

15. (Currently Amended) The ~~computer program product~~ program storage device of claim 13, wherein the plurality of outliers in the distribution of the set of historical data are identified by analyzing the set of historical data using statistical modeling, outlier analysis, and data mining algorithms.

16-18. (Canceled)

19. (Currently Amended) The ~~computer program product~~ program storage device of claim 13, wherein the set of updated data includes at least one of demographic data, psychographic data, transactional data, and environmental data.

20. (Currently Amended) The ~~computer program product~~ program storage device of claim 13, wherein generating the adjusted fence include:
adding the one or more new control points to the adjusted fence.

21. (Currently Amended) The ~~computer program product~~ program storage device of claim 13, wherein generating the adjusted fence include:
changing one or more of the plurality of control points to the one or more new control points in the adjusted fence.

22. (Currently Amended) The ~~computer program product~~ program storage device of claim 13, further comprising:

determining whether the adjusted fence, within the at least one data model, reached a steady state;

converting the adjusted fence to a static model in response to a determination that the adjusted fence reached the steady state; and

refining the at least one data model for an iteration of the plurality of iterations in response to a determination that the adjusted fence has not reached the steady state.

23. (Currently Amended) The ~~computer program product~~ program storage device of claim 22, wherein determining whether the adjusted fence reached a steady state includes:

determining a difference between the adjusted fence and a previous data model, within the at least one data model, to form a delta value; and

determining whether the delta value is less than a threshold.

24. (Currently Amended) The ~~computer program product~~ program storage device of claim 23, wherein the threshold is two standard deviations from a mean within a normal distribution of data.

25. (Currently Amended) An apparatus for detecting fraud, the apparatus comprising: a processor, and instructions stored in a memory, wherein the instructions are adapted to cause the processor to perform a plurality of steps comprising:

receiving a set of historical data stored in a customer behavior database;

identifying a plurality of control points in the set of historical data using a data analysis module, further comprising:

performing a statistical analysis on the set of historical data for identifying a plurality of outliers, wherein the plurality of outliers are identified by the statistical analysis as a set of significantly different data points in a distribution of the set of historical data; and

performing data mining techniques on ~~validating~~ the plurality of outliers to distinguish between a first set of outliers and a second set of outliers, wherein the first set

of outliers are classified by the data mining techniques as ~~valid~~-non-fraudulent outliers and the second set of outliers are classified by the data mining techniques as ~~invalid~~ fraudulent outliers, and wherein the first set of outliers are identified as the plurality of control points;

building at least one data model based on the plurality of control points, further comprising:

generating a fence that passes through the plurality of control points to define a boundary between data points, wherein the fence comprises line segments connecting the plurality of control points to form a continuous line for the boundary, and wherein data points inside or on the boundary of the fence represent acceptable behavior and data points outside the boundary of the fence represent fraudulent behavior;

receiving a set of updated data, wherein the set of updated data includes a plurality of current data stored in the customer behavior database;

identifying one or more new control points based on the set of updated data using the data analysis module, further comprising:

performing a statistical analysis on the set of updated data for identifying an additional plurality of outliers, wherein the additional plurality of outliers are identified by the statistical analysis as an additional set of significantly different data points in a distribution of the set of updated data; and

performing data mining techniques on ~~validating~~ the additional plurality of outliers to distinguish between a third set of outliers and a fourth set of outliers, wherein the third set of outliers are classified by the data mining techniques as ~~valid~~-non-fraudulent outliers and the fourth set of outliers are classified by the data mining techniques as ~~invalid~~-fraudulent outliers, and wherein the third set of outliers are identified as the one or more new control points;

adjusting the at least one data model to form an adjusted fence, within the at least one data model, based on the one or more new control points, wherein the at least one data model is refined for a plurality of iterations, further comprising:

generating the adjusted fence that passes through the plurality of control points and the one or more new control points to define a new boundary between data points, wherein the adjusted fence comprises line segments connecting the plurality of control

points and the one or more new control points to form a new continuous line for the new boundary, and wherein data points inside or on the new boundary of the adjusted fence represent acceptable behavior and data points outside the new boundary of the adjusted fence represent fraudulent behavior; and
verifying a transaction based on the adjusted fence.